IMPLEMENTASI KRIPTOGRAFI AES DAN OTP DALAM MEMBANGKITKAN KODE OTENTIKASI UNTUK AKTIVASI *ONLINE MEMBER* BARU YANG DIKIRIM MELALUI SMS

ABSTRAK

Pembuatan Akun palsu yang digunakan untuk perbuatan tidak baik sangat merugikan dan membuat buruk citra pemilik dan situs media sosial atau situs jual beli online miliknya, oleh karena itu diperlukan tindakan pencegahan agar pengguna tidak mendaftarkan akun palsu, caranya dengan menggunakan kode otentikasi yang berisi pesan aktivasi akun yang hanya sekali pakai dan memiliki jangka waktu pakai dengan mengimplementasikan metode *One-time Password* dan dikirimkan melalui SMS pada nomor telepon seluler pengguna. Kode otentikasi ini dibangkitkan dengan menggunakan algoritma kriptografi Advance Encryption Standard. Namun karena pada tahun 2011, tiga orang peneliti dari beberapa Universitas dan Microsoft menemukan adanya celah pada enkripsi AES. Maka kompleksitas dari AES ini perlu ditingkatkan dengan cara memodifikasinya untuk menutupi celah yang ditemukan, pemodifikasian AES dapat dilakukan pada bagian S-Box dan ShiftRow, sehingga S-Box dan ShiftRow yang digunakan akan dinamis mengikuti kunci yang diberikan. AES-256bits dipilih karena memiliki jumlah kombinasi kunci lebih banyak dan waktu yang dibutuhkan untuk membongkar pesan lebih lama. Setelah pemodifikasian AES-256bits dibuat maka tahapan selanjutnya adalah menguji hasil modifikasi AES-256bits dengan Avalanche Effect dan Randomness Test, dimana algoritma kriptografi yang baik memiliki nilai Avalanche Effect yang berada disekitar 50% dan lolos pengujian 5 dasar uji keacakan pada RandomnessTest.

Kata Kunci: Kriptografi, AES, OTP, Kode Otentikasi.

IMPLEMENTATION OF CRYPTOGRAPHY AES AND OTP TO GENERATE AUTHENTIC CODE SENT VIA SMS FOR NEW MEMBER ONLINE ACTIVATION

ABSTRACT

Fake Account Creation used for bad deeds is very harmful and denigrate the owners and social media or marketplace, therefore it's necessary to take preventive action so that the user does not register a fake account, one of the ways is to use the authentication codes which contain an activation message account that only disposable and have a specific lifetime by implementing One-time Password methods, tehe authentication codes sent via SMS to the user's mobile phone number. This authentication code generated using a cryptographic algorithm Advanced Encryption Standard. However in 2011, three researchers from several universities and Microsoft find the crack in the AES encryption. one of solutions to improved the complexity of this AES is by modifying it to cover a crack, modifying AES can be performed on the S-Box and ShiftRow, so that the S-Box and ShiftRow used will dynamically depend to the given key. AES-256bits chosen because it has more number of key combinations and need more time to decrypt messages. After modifying AES-256bits made then the next step is to test the modified AES-256bits with Avalanche Effect and Randomness Test, which has a good cryptographic algorithms Avalanche Effect value that was around 50% and passed the test five basic randomness test on RandomnessTest.

Keywords: Cryptography, AES, OTP, Authentication Code.